The Software Alliance

BSA

BSA Global Best Practices for Law Enforcement Access to Digital Evidence

As the types and volume of data proliferate, digital evidence is increasingly important to law enforcement agencies. While the value of digital evidence to criminal investigations has grown substantially, so, too, have challenges in accessing it. Incomplete legal structures, insufficient law enforcement capacity, and underdeveloped investigatory processes often hamstring investigations and create unnecessary tension between law enforcement agencies and technology providers. Policymakers, law enforcement agencies, and technology providers should work collaboratively to shape laws, policies, and procedures that enable access to digital evidence in alignment with robust protections for due process and civil liberties, and that ensure providers can meet their obligations to their customers.

BSA recommends the following best practices relating to law enforcement access to digital evidence for policymakers, law enforcement agencies, and technology providers. These best practices promote strong commitments to privacy, security, transparency, and the rule of law, while fostering constructive collaboration between law enforcement and technology providers in activities aimed at fighting crime and making communities safer.

Best Practices for Governments and Law Enforcement Agencies

Law enforcement agencies have access to more data than at any time in history. Accessing that data can present tremendous challenges to the privacy and security of technology users unless law enforcement investigations are guided by carefully crafted laws, policies, and procedures. BSA recommends the following best practices to policymakers and law enforcement agencies. The best practices would empower criminal investigators to access digital evidence without compromising the security of the technology or the safety, rights, and opportunities of citizens. The best practices are organized around five guiding principles: safeguarding fundamental rights, narrowly targeting requests, cooperating across borders, ensuring transparency, and maintaining collaborative relations with technology providers.

THE RISING IMPORTANCE OF DIGITAL EVIDENCE

Over the last 30 years, data sources have exploded. Billions of individuals have moved from telephone and written communications to digitally transmitted and stored emails, text messages, phone calls, instant messages, social media postings, and other communications. The European Commission now estimates that electronic evidence is needed in roughly 85 percent of criminal investigations, and in more than half of all criminal investigations law enforcement agencies require access to electronic evidence stored outside their country's borders. In the US, the Federal Bureau of Investigation has found that the average digital forensic examination can yield nearly a terabyte of data — equivalent to 250,000 pages of typewritten documents.

Safeguarding Fundamental Rights

The first obligation of governments and law enforcement agencies is to the citizens they protect. Laws and policies should ensure that safeguards for the rights and liberties of citizens are incorporated at all stages of law enforcement investigations involving digital evidence.

Judicial Review. Laws should ensure that prior review by an independent judicial authority is available for any order (1) authorizing government access to content data, other sensitive data, or technologies produced or controlled by technology providers, or (2) mandating that technology providers take specific actions impacting data or technologies. Technology providers subject to such an order should have the opportunity to challenge it before an independent judicial authority based on factors relating to feasibility, legality, propriety, and international comity.

Privacy. Laws should establish robust substantive and procedural protections for privacy and civil liberties in connection to data requests and their fulfillment, including measures to protect fundamental rights to free speech and expression; prevent extralegal search and seizure of digital evidence; bar use of unlawfully obtained evidence in criminal proceedings; and prohibit bulk collection of content data.

Due Process. Laws should protect due process, including the right to fair trial, the presumption of innocence, prohibitions against arbitrary arrest and detention, and judicial redress.

Emerging Technologies. Emerging technologies often create new data sources not anticipated by existing policies. Policymakers should continue to update laws to ensure emerging technologies and associated data are covered by the same robust privacy and due process protections as traditional sources. Data from facial recognition technologies, home assistant software, and medical Internet of Things devices offer current examples of emerging data sets that should be covered by protections similar to those generally afforded to content information.

Narrowly Targeting Requests

Law enforcement agencies should target requests only to information vital to an investigation and develop such requests through appropriate legal processes. Doing so not only builds confidence among citizens in the authorities and activities of the investigators but also improves the efficiency and effectiveness of the investigations themselves.

Specificity. Laws should require that a request for data be as specific and narrowly targeted as possible. It should articulate details about specific individuals, accounts, devices, and types of data to be targeted, and a specific time period over which they will be targeted. Requests should always be issued in connection to investigation of a specific crime, and should include a reasonable justification based on credible and articulable facts.

Content vs. Non-Content. With regard to accessing stored data, laws should create a distinction between content data and non-content data, and tailor legal processes to each category in ways that ensure robust due process and privacy protections. Content data includes the content of an electronic exchange. It requires special safeguards because of the particularly intrusive and sensitive impact of third-party access to that data. Non-content data encompasses subscriber data (information on the identities of the senders and recipients of an electronic exchange) and traffic data (metadata including the timing, frequency, and duration of such an exchange).

Real-Time Access. Laws should establish a high procedural threshold for authorizing real-time access to traffic data, conduct of remote searches, and interception of content data; such access should require a search warrant or equivalent order approved by an independent judicial authority.

Minimization. Laws should require that law enforcement agencies adopt minimization procedures in connection with requests for access to data to ensure that only relevant data is produced and used. Minimization procedures should be applied to the acquisition of data to ensure that only that data relevant to an investigation is produced in

response to a request. Minimization procedures should be applied to the processing, retention, and dissemination of data acquired through requests in order to ensure that (1) data acquired by the law enforcement agency that is not relevant to the specific investigation for which it was required is returned or destroyed; (2) such data is only used for lawful purposes; and (3) data is secured against unauthorized access or disclosure.

Cooperating Across Borders

Cross-border cooperation is necessary to enable law enforcement agencies to access data, which is increasingly stored in facilities dispersed around the world. Moreover, such cooperation provides mechanisms to reinforce procedural protections and legal safeguards.

Comity Analysis. Policymakers should ensure that their governments have a process in place to identify potential conflicts of law prior to the issuance of requests, incorporate comity analysis into judicial proceedings regarding the issuance and enforcement of requests, and provide opportunities for impacted stakeholders to provide comity analyses relevant to their position in such proceedings.

Notification. Governments should notify a foreign country — either where the data is located or where the person of interest resides — when its law enforcement agencies are requesting access to digital evidence stored in the foreign country, and to grant the foreign country and technology provider the opportunity to object.

International Agreements. Governments should establish procedures and mechanisms for accepting and responding to requests under mutual legal assistance treaties on a timely basis, including, where feasible, digital portals for accepting requests. In addition, to the extent feasible, governments should establish or negotiate other mechanisms, including bilateral and multilateral international agreements, to facilitate cross-border law enforcement access to data under appropriate circumstances.

Data Localization. Policymakers should avoid data localization mandates for the purposes of ensuring law enforcement access to data, to avoid myriad unintended negative consequences data localization policies often generate. The data storage location should not be the governing factor in establishing jurisdiction or access rights.

Ensuring Transparency

Transparency is vital for sustaining public confidence in the authorities granted to law enforcement agencies and the conduct of the agencies in executing those authorities.

Notification of Data Subjects. Technology providers should not be restricted from notifying the subject of a data request unless non-disclosure is justified on an exceptional basis for a limited duration. Procedures should ensure that technology providers have the right to request further information or object when such notification is prohibited.

Public Reporting. As a matter of practice, governments should regularly publish aggregate data on the number, purposes, legal authorities, and outcomes of law enforcement requests for digital evidence issued by law enforcement agencies in a covered timeframe. Technology providers should not be restricted from publishing aggregate data on the number, origin, and outcomes of law enforcement requests for digital evidence they receive in a covered timeframe.

Maintaining Collaborative Relations With Technology Providers

Building collaborative relationships that recognize the equities of all stakeholders involved provides the most effective way to ensure sustainable, effective mechanisms to access digital evidence in accordance with the law.

Controllers vs. Processors. When requesting access to digital evidence, law enforcement agencies should seek data first from the data controllers, which determine the means and purposes of processing personal data, before going to data processors, which process data on behalf of data controllers.

Technical Capabilities. Technology providers should not be required, under any circumstances, to alter or weaken technologies, or to build or modify technical capabilities, in ways that risk creating systemic weaknesses or vulnerabilities. Specifically, no law or policy should obligate technology providers to create access to security technologies such as encryption mechanisms, to implement technical measures to enable law enforcement to access encrypted communications, or to maintain a capability to decrypt protected communications.

Rights of Technology Providers. Laws should establish that technology providers cannot be held liable for responding to lawful government requests for data and should include protections to prevent intellectual property, trade secrets, and other proprietary and sensitive information (including source code) from being exposed as a result of law enforcement requests.

Request Verification. Law enforcement and government agencies should ensure that request recipients are able to establish viable processes to verify the validity and accuracy of law enforcement requests for data.

BSA Recommendations for Technology Provider Best Practices

Technology providers play an important role in responding law enforcement efforts to requests for digital evidence in criminal investigations, but legal and procedural shortcomings can also undermine their ability to do so. Providers are obliged to protect the trust and confidence of their customers, including in relation to customer privacy and security, and cooperation with criminal investigations should not compromise these investigations.

Not all technology providers receive law enforcement requests in significant numbers; but those that do should follow best practices described below to improve responsiveness to legitimate law enforcement requests while sustaining commitments to customers around privacy and security.

Accessibility and Standardization. Technology providers should maintain a clearly identifiable online mechanism to receive law enforcement requests for data and to provide dated, electronic confirmation of receipt of the request. Technology providers should also strive to standardize request forms.

Responsiveness. Technology providers should establish a policy requiring, absent exceptional circumstances, an initial response to general law enforcement requests within a reasonable and defined timeframe. The policy should also outline expectations for accelerated response to designated law enforcement requests in exigent circumstances involving danger of death or serious physical injury to any person.

Point of Contact. Technology providers should identify a single point of contact or contact mechanism that ensures accountability for the processing of and response to law enforcement requests. Further, they should maintain a mechanism for law enforcement agencies to communicate promptly with appropriate personnel in the event of an emergency.

Guidance. Technology providers should maintain and make public up-to-date, complete guidance on the types of data law enforcement agencies may access with appropriate authorization and the procedures for accessing it.

Training. Technology providers should, where relevant, provide training to law enforcement agencies at the federal, state, and local level and to prosecutors and judges on the types of data that may be available via their platforms or services, methodologies for appropriately specifying data requirements, considerations about privacy and feasibility, and other relevant matters.

Notification. Absent exceptional circumstances, including imposition of non-disclosure requirements by a requesting government, technology providers should notify data subjects when they receive a law enforcement request for the data subject's data.

Privacy. Technology providers should establish policies and mechanisms to prevent over-responsiveness; customers' data should be provided to law enforcement agencies only in connection to legitimate criminal investigations and only in response to properly authorized requests made in accordance with appropriate laws and court orders. Only the information that is relevant to and specifically authorized by their submitted request should be provided.